# Huntsman
Threat Intelligence

Huntsman®
Defence-Grade Security Platform

Huntsman Threat Intelligence allows organisations to interpret events in the context of known threat fingerprints or profiles. It does this automatically, and in real time.

Huntsman Threat Intelligence sources cyber security intelligence and event context from:

- **External sources**
  A public or commercial list of compromised websites or botnet members
- **Community-based sources**
  Such as a CERT service or an industry body
- **Localised and specific sources**
  Based on either known risk factors; sensitive systems, users or networks; or specific actionable intelligence sources
- **Contextual sources**
  Such as ongoing investigations or other systems.

So, rather than simply mirroring "siloed" external sourced information, Huntsman ingests external threat intelligence together with internal observations to automate the analysis of the broader threat information for richer situational awareness and event contextualization.

This delivers unparalleled real-time clarity about threats, their severity and likely impact – and significantly improves the quality of security decision-making.

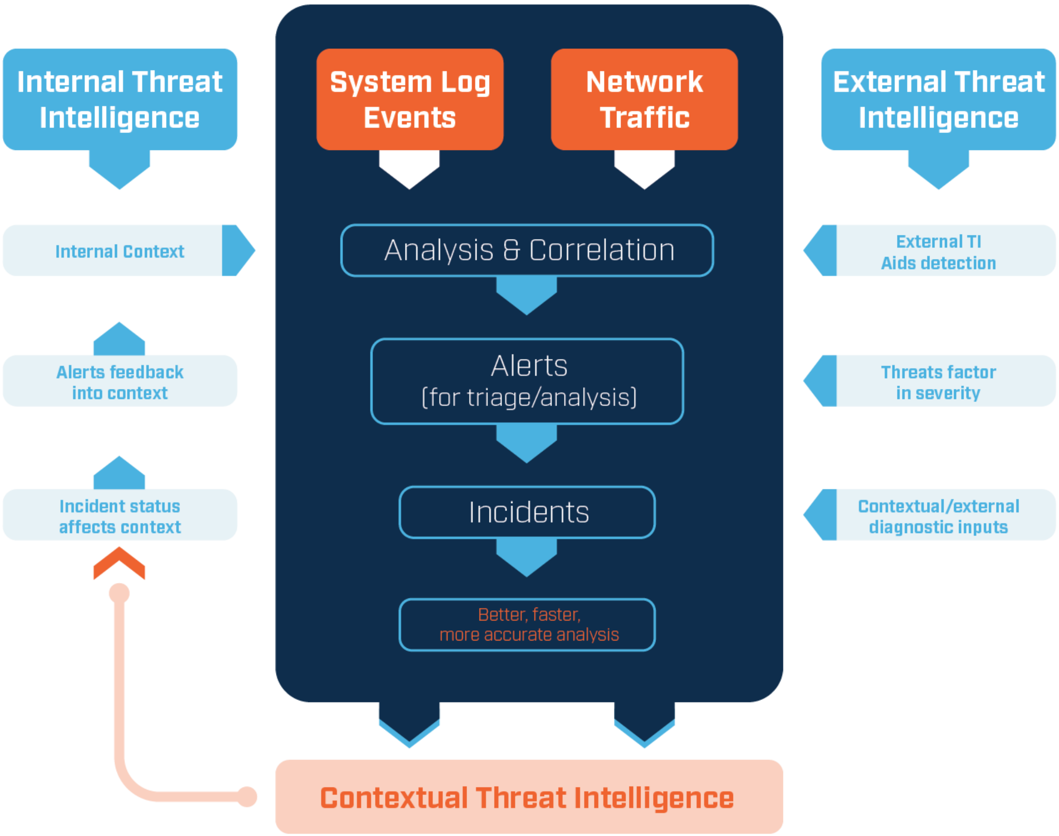
Huntsman Threat Intelligence is an add-on for the Huntsman Enterprise SIEM (including the Cloud Edition) and Unified Console. It is included in the MSSP Edition.

### HUNTSMAN ENTERPRISE SIEM FEATURES:

- Automated threat analysis process
- Support for a range of information sources and data types
- Vendor-neutral capability to collect intelligence from a range of sources
- Create feedback from alerts to enable new threat information to automatically update internal reference data
- Alert on repetitions of known incidents
- Detect changed patterns of misuse across systems or a user population
- Model of user and asset risk and sensitivity to support detection, diagnosis and incident resolution

### ADDITIONAL CLOUD EDITION FEATURES:

- Reduced time to threat resolution
- More accurate, real-time detection of security incidents
- Better determination of the meaning, significance, relevance and severity of alerts
- Faster decision-making
- Dynamic awareness between internal systems, real-time threat detection controls and localised 'threat context'
- Reduced risk and improved cyber resilience


Internal Threat Intelligence
System Log Events
Network Traffic
External Threat Intelligence
Internal Context
Analysis & Correlation
External TI Aids detection
Alerts feedback into context
Alerts (for triage/analysis)
Threats factor in severity
Incident status affects context
Incidents
Contextual/external diagnostic inputs
Better, faster, more accurate analysis
Contextual Threat Intelligence

## THE ADVANTAGES OF THREAT INTELLIGENCE

Applying knowledge of the outside world, wider threat landscape and internal context and risk factors provides significant advantages in detecting attacks and aids the decision making process around alerts and incidents through verified, referenceable information and intelligence.

## BETTER DETECTION

When it comes to cyber attacks or internal cases of insider misuse the speed of detection is key – enabling understanding, containment and resolution to start before an infection has spread or data losses have become too severe.

- **Reduced time to threat resolution**
  Huntsman analyses and triages the relevant information to contextualise and validate genuine alerts and eliminate false positives
- **More accurate, real-time detection of security incidents**
  Huntsman enables new threat intelligence information to be correlated with internal events

## BETTER UNDERSTANDING

When an alert is raised it is often difficult for analysts to accurately and confidently diagnose the true nature of the breach.

This understanding is vital to ensure that real problems can be dealt with and escalated or that manageable problems can be swiftly acknowledged or resolved.

The process is often hampered by a lack of information or context for the decision to be based on.

- **Better determination of the meaning, significance, relevance and severity of alerts**
  Huntsman gives an operator greater situational awareness and better information so they can make an informed decision

## IMPOVED RESPONSE TIME

When a breach is understood it is important to respond quickly and effectively. For example, if a piece of malware has infected a single user the response might be to quarantine the user and despatch a support engineer. If that same piece of malware has infected thousands of users the response will be different.

Correctly making these decisions based on internal and external reference data and context plays a big role in getting this right.

- **Faster decision-making**
  Huntsman automates the collection and analysis of threat information without requiring manual data gathering and analysis
- **Dynamic awareness between internal systems, real-time threat detection controls and localised 'threat context'**
  Huntsman enables real-time detection and diagnosis of attacks that traverse the 'kill chain'

## IMPROVED CYBER RESILIENCE AND REDUCED RISK

Cyber resilience is about risk reduction in terms of likelihood, vulnerability and impact.

Having good awareness of known external and internal threats, being able to decide quickly what is important and knowing that your teams can confidently respond all add to the overall cyber resilience of the organisation.

Huntsman reduces risk resulting from incomplete or non-current threat intelligence during the detection, investigation or resolution processes.

**Huntsman | Tier-3 Pty Ltd**

**Asia Pacific**
t: +61 2 9419 3200
e: info@huntsmansecurity.com

Level 2, 11 Help Street
Chatswood NSW 2067

**EMEA**
t: +44 845 222 2010
e: ukinfo@huntsmansecurity.com

100 Pall Mall, St James
London SW1Y 5NQ

**North Asia**
t: +81 3 5809 3188
e: info@huntsmansecurity.com

TUC Bldg. 7F, 2-16-5 Iwamoto-cho,
Chiyoda-ku, Tokyo 101-0032

**Americas**
toll free: 1-415-655-6807
e: usinfo@huntsmansecurity.com

Suite 400, 71 Stevenson Street
San Francisco California 94105

huntsmansecurity.com

linkedin.com/company/tier-3-pty-ltd

twitter.com/Tier3huntsman